UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

FEDERAL INSURANCE COMPANY,

Plaintiff, : Case No. 2:17-cv-135

-vs- Judge Sarah D. Morrison
Magistrate Judge Elizabeth Preston Deavers

BENCHMARK BANK,
:
Defendant.

OPINION AND ORDER

This matter is before the Court on cross-motions for summary judgment filed by Plaintiff Federal Insurance Company and Defendant Benchmark Bank. (ECF Nos. 51, 53). For the reasons that follow, the Court **DENIES** Plaintiff's Motion and **DENIES IN PART** and **GRANTS IN PART** Benchmark's Motion.

I. BACKGROUND

Non-party Woda Cooper Companies, Inc. ("Woda"), formerly known as Valhalla Management & Real Estate, LLC, dba Woda Management, develops low income affordable housing in the form of apartment communities. (George Depo., 23, ECF No. 45; ACH Agreement, ECF No. 1-2). At the relevant time, Woda operated as the parent company to three subsidiaries—Woda Cooper Development, Woda Construction, Inc. ("WCI"), Woda Management & Real Estate, LLC—and managed several hundred affiliates through limited partnerships, including Mary Harvin Center Limited Partnership and Boury Lofts Limited Partnership (the "Limited Partnerships"). (George Depo., 38, 118; Ferrell Depo., 10–14, ECF No. 47). Woda is owned by managing directors David Cooper, Jr. and Jeffrey Woda. (George Depo., 18–19, 43). Plaintiff Federal Insurance Company ("Plaintiff") is the subrogee of the

Limited Partnerships. (Phair Aff., ¶ 6, ECF No. 53-1).

A. Woda's Banking Relationship with Benchmark

On March 28, 2011, Woda entered into a Business Online Access Banking Agreement ("Banking Agreement") with Defendant Benchmark Bank ("Benchmark") to provide Woda with electronic banking access for various commercial accounts under its control. (ECF No. 1-3). At that time, Mr. Cooper and Mr. Woda were both on Benchmark's Board of Directors. (George Depo., 60–61; Caldwell Decl., ¶ 3, ECF No. 51-2). Woda established hundreds of banking accounts at Benchmark, including for the Limited Partnerships and WCI. (Caldwell Decl., ¶ 7).

On the same date, Woda also entered into an ODFI-ACH Originator Agreement ("ACH Agreement") with Benchmark, allowing Woda to initiate online ACH transfers for designated accounts listed in Schedule C. (ECF No. 1-2). Laura George (Vice President and Controller at Woda) was named as the company-authorized representative with respect to security procedures in the Agreement. (*Id*. Scheds. B, C). Schedule C was never formally amended after March 28, 2011. (George Depo., 105–06). But it was Benchmark's understanding that all Woda accounts that were added after March 28, 2011 and requested ACH access, including the Limited Partnerships, would fall under the original ACH Agreement—there did not need to be a new or updated Schedule C each time an authorized account was added. (Vincent Depo., 89–92, ECF No. 43; Caldwell Decl., ¶ 8). Pursuant to the Agreement, ACH transfers were only delivered through the internet banking system. (ACH Agreement, Sched B). Woda declined the delivery options of 3.5-inch diskette, manual report, and any "other" mechanism. (*Id*.). The maximum limit on the dollar amount of single ACH transfers was $50,000. (*Id.* Sched C).

B. Benchmark's Security Procedures

After the Agreements were signed, Ms. George met with Jan Vincent (a Business Banker at Benchmark), and Jerry Caldwell (Chief Executive Officer, Chairman, and President of Benchmark) to establish parameters for Woda's online banking with Benchmark.[1] (Vincent Decl., ¶ 4, ECF No. 51-4; Vincent Depo., 10–11, 49; George Depo., 65–66; Caldwell Decl., ¶ 2). Following this discussion, one unique username and password was assigned to each Woda employee who was granted access to any Woda bank accounts. (George Depo., 73–74; Vincent Decl., ¶ 6). Each employee also had to set up security questions and answers that were triggered by a risk score algorithm. (George Depo., 86; Caldwell Decl., ¶ 6). Although Fiserv usually generated temporary passwords for new accounts, there was at least one occasion where Mr. Caldwell sent Ms. George an e-mail that listed generic temporary passwords for new Woda users. (Vincent Depo., 128–29; Ex. F., ECF No. 44-4;). At some point, Ms. Vincent or Mr. Caldwell also offered Ms. George banking tokens as an additional security feature. (George Depo., 79; Vincent Depo., 50–52; George Aff., ¶ 11, ECF No. 53-3). However, when Ms. George was told that Woda did not have to use tokens, she declined because they were "inconvenient." (George Depo., 137–38).

Upon any attempted log in, Fiserv's software would verify that the username, password, and security questions, if prompted, were correct. (Vincent Depo., 36). If someone tried to log in with bad credentials, they would be locked out after three unsuccessful attempts. (*Id.*). Benchmark would then get a Fiserv report the next day that showed any log in attempts and account lockouts. (*Id.* at 37). Fiserv utilized IP blacklisting as well. (Vincent Decl., ¶ 6).

In addition to these security measures, ACH transfers required dual authorization. (George Depo., 75, 91–92). This allowed Woda to assign users who could initiate ACH transfers but then require another approved internal user to authorize the transfer before funds

[1] Benchmark's online banking platform was provided by Fiserv, Inc. (Vincent Depo., 20).

were released to Benchmark to either reject or approve the request. (Vincent Depo., 54–56). However, at Woda's request, designated employees could bypass dual authorization and both initiate and approve ACH transfers. (George Depo., 78, 93; Vincent Decl., ¶ 7). Benchmark's Board of Directors set out the procedures and policies for the bank, including the required security procedures and the ACH policy. (Vincent Depo., 44; Decl. Caldwell, ¶ 9; Ex. B, ECF No. 44-2).

Part of Ms. Vincent's job was to assist Benchmark customers, including Woda, in generating ACH transfers through the online banking system. (Vincent Depo., 30–32). Ms. Vincent would designate specific individuals as ACH users per instructions from the customer. (*Id.* at 38). This included filling in each person's online banking profile with their personal data, e-mail, what accounts they had access to, and any accounts "they would be signers on." (*Id.* at 40). In approving or rejecting an ACH request, Ms. Vincent would look to see if the ACH transfer was generated by a known authorized user, the debits and credits balanced, and the account the user was transferring money from had money in it to cover the transfer. (*Id.* at 31; ACH Agreement, ¶ 2(a)). If the ACH transfer met this criterion, Ms. Vincent would release the funds to the designated recipient. (Vincent Depo., 31).

Ms. George was one of the supervisors responsible for managing the list of Woda employees who had access rights to bank accounts at Benchmark, including who could initiate and/or approve ACH transfers and from which accounts. (George Depo., 72, 89). Ms. George communicated any changes to that list to Ms. Vincent by e-mail, phone, and/or in person. (*Id.* at 72–73; Vincent Depo., 97). As long as the request for access came from Ms. George, Jill Clifford (Development Controller), or Amy Brown (Head of Accounting), Ms. Vincent would make the necessary authorization. (Vincent Depo., 76). While Ms. Vincent relied on Ms. George to keep her apprised of which Woda employees should have ACH access and to what accounts, Ms. Vincent would sometimes initiate a check to see if Woda had any new personnel who should have ACH access or if anyone left and their account should be terminated. (*Id.* at 74). According to Ms. George, Woda had a high, almost daily, rate of employee turnover among all its subsidiaries and affiliates. (*Id.* at 74; George Depo., 107–10; Ex. 5, ECF No. 46-2).

C. The Fraudulent Transfers

On March 22, 2016, Ms. Clifford emailed Ms. Vincent to request that Donna Ferrell, WCI's Director of Accounting–Construction, be given access to view and process ACH transfers for WCI's account. (Ex. 7, ECF No. 46-4). Donna Ferrell replaced Sue Milner. (Ferrell Depo., 10). At some point either before or after this e-mail, Ms. George also told Ms. Vincent to "duplicate [Sue Milner's] rights with respect to activities that she could perform, but not necessarily access rights to properties that Sue had access to." (Ex. 7, ECF No. 46-4).

Ms. George later confirmed to Mr. Woda that Ms. Ferrell did have the ability to bypass dual authorization and initiate and approve ACH transfers for processing. (George Depo., 122–23, Ex. 8, ECF No. 46-5). However, Ms. George says that no one ever authorized Benchmark to give Ms. Ferrell access to the Limited Partnership accounts, "much less the ability to process ACH transfers from these accounts." (George Aff., ¶¶ 14–15). Yet, according to Ms. Vincent, she was asked to designate the Limited Partnership accounts as "construction accounts" with both online banking and ACH access and to give the entire Woda accounting group access to the accounts. (Vincent Decl., ¶¶ 8–9). Moreover, Ms. Vincent alleges that both Ms. Clifford and Ms. George specifically requested on separate occasions that Ms. Ferrell be given access to the Limited Partnership accounts, including ACH authorization. (*Id.* ¶ 11; Vincent Depo., 105–07). Ms. Ferrell believed she only had access to the WCI account at Benchmark. (Ferrell Aff., ¶¶ 8–9, ECF No. 53-6).

On May 18, 2016, Ms. Ferrell attempted to log in to her Benchmark account from her Woda computer but was notified that she was locked out. (Ferrell Depo., 34). Another employee, Terri Myers, attempted to log in to her own Benchmark bank account on Ms. Ferrell's computer but was also unable to do so. (*Id*. at 36). However, Ms. Ferrell and Ms. Myers were able to log in to their respective Benchmark accounts on Ms. Myers' computer. (*Id.* at 36–37). In doing so, Ms. Ferrell was able to initiate a legitimate ACH transfer using her Benchmark account. (*Id.* at 38–39).

Ms. Ferrell then called Ms. Vincent and left a voicemail about the lockout notification. (Vincent Depo., 138–39; Ex. I, ECF No. 43-10). After Ms. Vincent listened to the voicemail, she logged into Benchmark's access manager, looked at Ms. Ferrell's account, and noted that there were no log in attempts or lockouts on her account. (Vincent Depo., 139–40). Ms. Vincent then left Ms. Ferrell a voicemail indicating that Ms. Ferrell was not locked out of her account, she had not changed Ms. Ferrell's password, but that she "went ahead and unlocked the questions and things," and directed Ms. Ferrell to try to log in again. (*Id.* at 139, 141–43). According to Ms. Vincent, she did not actually "unlock anything because nothing was locked out," she was just trying to "give [Ms. Ferrell] confidence that the security questions were unlocked, her password was unlocked, she should try again." (*Id.* at 144–45). Ms. Ferrell was able to log in to her Benchmark account on her own Woda computer the next day with no problems and without any change to her username or password. (Ferrell Depo., 38). At that time, all of the accounts she had access to appeared normal and her ACH transfer from the day before had processed. (*Id.* at 43–44). When Ms. Vincent received an ACH transfer initiated and approved by Ms. Ferrell's account on May 18, she concluded that the issue had been resolved. (Vincent Depo., 145–47, 151–52).

On May 25 or 26, Ms. Vincent received a call from Wells Fargo requesting to verify an ACH transfer from Benchmark. (Vincent Depo., 152–53). Ms. Vincent confirmed that there was an ACH transfer approval by Ms. Ferrell's account matching the description given but indicated to Wells Fargo that she would check with Woda "just to verify." (*Id.* at 153–54). Ms. Vincent called Ms. George who responded that she had also received a call from Wells Fargo about the same thing. (*Id.* at 154–56; George Depo., 124–25). Ms. George told Ms. Vincent she was going to "check and see all of Donna's transfers and get back to [her]." (Vincent Depo., 156).

Ms. Vincent did not hear back from Ms. George. (*Id.*). Instead, shortly after their conversation, Ms. Vincent learned from Mr. Caldwell that "third-party criminals" made several unauthorized ACH transfers from the Limited Partnership accounts between May 18 and May 24 using Ms. Ferrell's credentials. (Vincent Decl., ¶ 13). Ms. Vincent and other Benchmark employees immediately began initiating reversals of the affected ACH transfers, including those fraudulently sent to Wells Fargo. (*Id.* ¶ 15; Vincent Depo., 157–60).

According to Ms. Vincent, she processed the fraudulent ACH transfers the same way she processed all ACH transfers. (Vincent Depo., 149, 179). She did not notice anything unusual about the dollar amounts of the fraudulent transfers, which were all between $26,328.00 and $83,217.00, as she had observed legitimate single ACH transfers approved by Ms. Ferrell for as high as $2,419,540.14. (Vincent Decl., ¶ 14; Woda Aff., ¶¶ 15–27, ECF No. 53-2).

Around the same time, Mr. Woda alerted Ms. Ferrell that someone had used her Benchmark username and password to make unauthorized ACH transfers out of the Limited Partnership accounts. (Ferrell Depo., 45–46). According to Ms. Ferrell, she kept her Benchmark login credentials on a sticky note in a locked drawer in her office. (*Id.* at 28). She did not write down the answers to her security questions. (*Id.* at 29). Ms. Ferrell subsequently contacted Woda's IT department, who took Ms. Ferrell's computer for examination. (*Id.* at 46–47).

According to Corey Daniels, a Woda IT Technician, malware was found on Ms. Ferrell's computer and the IP addresses of the hackers were traced to Virginia and Washington. (Ex. 15, ECF No. 47-5). Thereafter, Woda hired Rook Security, Inc. ("Rook") to conduct a forensic investigation and network vulnerability analysis of Woda's computer systems. (Ferrell Depo., 51, 57). In Rook's Vulnerability Analysis Report, it identified, among other things, that "two hosts were found running IPMI v.2.0 which contains an information disclosure vulnerability, allowing attackers to obtain password hashes." (Ex. 16, p. 19, ECF No. 47-6). Rook classified Woda's internal environment vulnerability as "high risk." (*Id.*).

Based on its review of Benchmark's log activity, Fiserv also believed that there was malware in the Woda network, which allowed intruders to obtain valid credentials for use in the ACH origination. (Ex. B, ECF No. 52-1). According to Fiserv, during the fraudulent transfers, Ms. Ferrell's credentials were used from two separate IP addresses at the same time, one originating from Columbus, Ohio and one from Washington State. (*Id.*). Neither IP address was blacklisted as a known bad IP address. (*Id.*). Fiserv did not detect any username or password data breach on its network nor did it have any records of recent accounts with stolen credentials from customers. (*Id.*). Finally, monthly vulnerability and penetration testing did not detect any intrusions. (*Id.*). Despite this information, Mr. Woda was convinced that the breach occurred at Benchmark or Fiserv and that "poor security practices at Benchmark allowed for [the] transfers." (*Id.*).

Ultimately, Benchmark was able to recover and return to Woda $197,708.00 of the $600,904.000 fraudulently transferred funds. (Vincent Decl., ¶¶ 13, 15; Woda Aff., ¶ 35).

Pursuant to a policy of insurance, Plaintiff paid Woda $500,000 for the loss, which included attorney's fees. (Phair Aff., ¶ 6). Upon taking assignment of Woda's claims against Benchmark, Plaintiff remains uncompensated for $403,196.00. (*Id*. at ¶¶ 5, 7).

D. Procedural History

The Limited Partnerships originally filed suit against Benchmark on July 7, 2016 in the Franklin County Court of Common Pleas, Case No. 16-CV-6417. On February 15, 2017, the Limited Partnerships voluntarily dismissed the state court action and filed suit in this Court. On May 24, 2017, Federal Insurance Company was substituted as the plaintiff and filed an Amended Complaint alleging five claims of relief: (1) breach of contract; (2) violation of the Ohio U.C.C.; (3) negligence; (4) violation of various federal statutes and regulations; and (5) conversion. (ECF No. 11). The Court has jurisdiction over this case pursuant to 28 U.S.C. § 1332(a)(1).[2] Following the Court's ruling (ECF No. 20) on Benchmark's Motion to Dismiss the Amended Complaint (ECF No. 12), only one claim remains: violation of the Ohio Uniform Commercial Code. Benchmark filed its Answer on February 7, 2018. (ECF No. 23).

On March 1, 2019, Plaintiff and Benchmark filed cross-motions for summary judgment (ECF Nos. 51, 53). On March 21 and 22, the parties filed their respective responses in opposition (ECF Nos. 54, 56), followed by reply briefs on April 4 and 5 (EC Nos. 57, 58). The cross-motions for summary judgment are now ripe for review.

II. STANDARD OF REVIEW

Summary judgment is appropriate when "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). The

[2] The Honorable Judge George C. Smith previously ruled that this Court can properly exercise diversity jurisdiction over this matter. (Opinion and Order, 7, ECF No. 20).

movant has the burden of establishing there are no genuine issues of material fact, which may be achieved by demonstrating the nonmoving party lacks evidence to support an essential element of its claim. *Celotex Corp. v. Catrett*, 477 U.S. 317, 322–23 (1986); *Barnhart v. Pickrel, Schaeffer & Ebeling Co.*, 12 F.3d 1382, 1388–89 (6th Cir. 1993). The burden then shifts to the nonmoving party to "set forth specific facts showing that there is a genuine issue for trial." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 250 (1986) (internal quotations omitted). When evaluating a motion for summary judgment, the evidence must be viewed in the light most favorable to the non-moving party. *Adickes v. S.H. Kress & Co.*, 398 U.S. 144, 157 (1970).

"When parties file cross-motions for summary judgment, the making of such inherently contradictory claims does not constitute an agreement that if one is rejected the other is necessarily justified or that the losing party waives judicial consideration and determination whether genuine issues of material fact exist." *B.F. Goodrich Co. v. U.S. Filter Corp.*, 245 F.3d 587, 593 (6th Cir. 2001). A genuine issue exists if the nonmoving party can present "significant probative evidence" to show that "there is [more than] some metaphysical doubt as to the material facts." *Moore v. Philip Morris Cos.*, 8 F.3d 335, 340 (6th Cir. 1993). In other words, "the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Anderson*, 477 U.S. at 248; *see also Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 597–98 (1986) (concluding that summary judgment is appropriate when the evidence could not lead the trier of fact to find for the non-moving party).

III. ANALYSIS

A. Requests to Strike Affidavits

In filing its Motion for Summary Judgment, Plaintiff attached affidavits of Maureen Phair, Jeffrey Woda, Laura George, David Hadley, Donna Ferrell, and Mat Gangwer (ECF Nos.

53-1–4, 53-6, 53-10). Benchmark argues that because the affidavits of Ms. Phair, Mr. Woda, Ms. George, and Ms. Ferrell were made "upon information and belief" they cannot be considered by the Court on summary judgment. Benchmark also argues that Mr. Gangwer's affidavit should be disregarded because it contains expert testimony from an undisclosed expert witness. In its Reply, Plaintiff responds that the disputed affidavits are based on the affiants' personal knowledge and should be considered. Plaintiff also disputes that Mr. Gangwer's affidavit constitutes expert testimony and argues it should be considered pursuant to Fed. R. Evid. 701.

On the other side, Plaintiff requests that the Court strike Benchmark's expert's report (ECF No. 51-5) because although Matthew Curtin was designated as Benchmark's rebuttal expert, he is "now its primary expert." (Pl. Brief Opp., 19, ECF No. 54). Benchmark responds that its reliance on Mr. Curtin's expert report is proper pursuant to Fed. R. Civil. P. 26(a)(2)(D)(ii).

1. Affidavits Made "Upon Information and Belief"

Pursuant to Fed. R. Civ. P. 56(c)(4), affidavits "must be made on personal knowledge, [and] set out facts that would be admissible in evidence." "'Magic words' are not required to make explicit that an affiant's declaration is based on personal testimony and competence" but rather, "a court can conclude from the context of the declaration whether those requirements are satisfied." *Ondo v. City of Cleveland*, 795 F.3d 597, 604 (6th Cir. 2015).

> [W]hen affidavits based on knowledge and belief are submitted to support or oppose a motion for summary judgment, the district court has discretion to determine whether it can differentiate between knowledge and belief for each averment in the affidavit. If the court can distinguish between the two, then . . . the court should excuse the affiant's stylistic error, and must admit the parts based solely upon personal knowledge, while striking the parts based upon belief. If the court cannot differentiate between the two, then . . . the court must strike the affidavit in its entirety[.]"

Id. at 605.

Upon review of the contested affidavits, it appears clear to the Court that despite the language used at the outset, each averment in each contested affidavit is made on personal knowledge. Moreover, the Court does not find that either Ms. George or Ms. Ferrell's affidavits conflict with their prior sworn deposition testimony, such that any portion of the affidavits should be disregarded on that basis. (Def. Brief Opp., 12–13, ECF No. 56); *see France v. Lucas*, 836 F.3d 612, 622 (6th Cir. 2016) ("[A]fter a motion for summary judgment has been made, a party may not file an affidavit that contradicts his earlier sworn testimony . . . unless the party opposing summary judgment provides a persuasive justification for the contradiction.") (internal quotations and citation omitted)). All four affidavits are admitted.

2. Expert Testimony vs. Lay Testimony

Pursuant to Fed. R. Evid. 701, a lay witness may only testify as to opinions or inferences which are "(a) rationally based on the witness's perception; (b) helpful to clearly understanding the witness's testimony or to determining a fact in issue; and (c) not based on scientific, technical, or other specialized knowledge within the scope of Rule 702." Put another way, "lay testimony results from the process of reasoning familiar in everyday life, whereas an expert's testimony results from a process of reasoning which can be mastered only by specialists in the field." *Harris v. J.B. Robinson Jewelers*, 627 F.3d 235, 240 (6th Cir. 2010) (internal quotations omitted).

Mr. Gangwer's affidavit (ECF No. 53-10) is not "lay testimony." While Mr. Gangwer's testimony is based on his own first-hand observation and review of Woda's computer network, nothing contained in the affidavit regarding computer security can arguably result from the process of reasoning familiar in everyday life. *See United States v. Ganier*, 468 F.3d 920, 926–27 (6th Cir. 2006) (explaining that while the average lay person may be able to interpret the outputs of computer software, the interpretation needed to make sense of the software reports requires specialized knowledge); *Goldman v. Healthcare Mgmt. Sys. Inc.*, No. 1:05-cv-035, 2008 WL 2462778, at *4–5 (W.D. Mich. June 11, 2008) (holding that a witness who performed a forensic analysis of the plaintiff's computer and wished to testify about the impact of his forensic examination on the computer was not offering lay testimony because such testimony would require scientific, technical, or other specialized knowledge). Rather, as stated ***by Mr. Gangwer***, he reached his opinion that "at the time of Rook's forensic investigation there was no malicious software identified on Ferrell's laptop which compromised her Benchmark Bank credentials . . . [b]ased upon [his] experience, education and knowledge of cybersecurity." (Gangwer Aff., ¶ 13). This is expert testimony as contemplated by Fed. R. Evid. 702.

Fed. R. Civ. P. 26(a)(2)(A) provides that "a party must disclose to the other parties the identify of any witness it may use at trial to present evidence under Federal Rule of Evidence 702, 703, or 705." "A party must make these disclosures at the times and in the sequence that the court orders." *Id.* 26(a)(2)(D). "If a party fails to provide information or identify a witness as required by Rule 26(a) . . . the party is not allowed to use that information or witness to supply evidence on a motion . . . unless the failure was substantially justified or is harmless." *Id.* 37(c)(1). Fed. R. Civ. P. 37(c)(1) requires absolute compliance with Rule 26(a). *Roberts ex. rel. Johnson v. Galen of Va., Inc.*, 325 F.3d 776, 782 (6th Cir. 2003).

The primary expert witness disclosure deadline in this case was November 1, 2018. (ECF No. 31). The rebuttal expert witness disclosure deadline was December 4, 2018. (*Id.*). Plaintiff does not contest that Mr. Gangwer was never disclosed as an expert witness. And Plaintiff's assertion that Mr. Gangwer's affidavit constitutes lay witness testimony does not prove that the failure was "substantially justified or harmless." *See Roberts*, 325 F.3d at 782 (noting that the burden is on the potentially sanctioned party to prove substantial justification or harmlessness); *Salgado v. General Motor Corps.*, 150 F.3d 735, 742 (7th Cir. 1998) (noting that the sanction of exclusion is automatic unless the sanctioned party can show the Rule 26(a) violation was either justified or harmless). Accordingly, the Court will disregard Mr. Gangwer's affidavit in ruling on the cross-motions for summary judgment.

3. Benchmark's Expert Report

From what the Court can gather from its Brief in Opposition, Plaintiff appears to be requesting that the Court strike Mr. Curtin's report because although he was timely disclosed as Benchmark's rebuttal expert (*see* ECF No. 37), he is now acting as a primary expert.

In his affidavit, Mr. Curtin attests that he has attached a true and accurate copy of his rebuttal report in response to Plaintiff's expert report prepared by David Hadley. (Curtin Aff., ¶¶ 3–4, ECF No. 51-5). Similarly, a review of Mr. Curtin's report appears to properly "contradict or rebut evidence on the same subject matter identified by" Mr. Hadley, pursuant to Fed. R. Civ. P. 26(a)(2)(D)(ii). Plaintiff's request is denied.

B Benchmark's Verification of the Fraudulent Payment Orders

Plaintiff asserts that it is entitled to recover Woda's $403,196.00 loss from Benchmark because the fraudulent payment orders were not effectively verified pursuant to Ohio Revised Code § 1304.57. (Amend Compl., ¶¶ 120–24, ECF No. 11). Section 1304.57, corresponding to section 4A-202 of the Uniform Commercial Code ("U.C.C."), provides in pertinent part:

> (B)(1) If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if both of the following apply:
>
> > (a) The security procedure is a commercially reasonable method of providing security against unauthorized payment orders.

> (b) The bank proves that it accepted the payment in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer.

In other words, the risk of loss for an unauthorized transfer initiated by a third party remains with Benchmark, unless Benchmark can show that "(1) the bank and customer agreed that the authenticity of payment orders would be verified pursuant to a security procedure; (2) the security procedure is commercially reasonable; and (3) the bank proves that it accepted the orders in good faith and in compliance with the security procedure and any written agreement or instruction of the customer." *Experi-Metal, Inc. v. Comerica Bank*, No. 09-14890, 2011 WL 2433383, at *1 (E.D. Mich. June 13, 2011) (construing Michigan's identically-worded U.C.C. provision at Mich. Comp. Laws § 440.4702).

1. Agreement Between Woda and Benchmark

The Court first considers whether Benchmark and Woda agreed that the authenticity of ACH payment orders would be verified pursuant to certain security procedures. Ohio Rev. Code § 1304.57(B)(1).

A "security procedure" is "a procedure established by agreement of a customer and a receiving bank for the purpose of verifying that a payment order . . . is that of the customer[.]" *Id.* § 1304.56. Only security procedures established by agreement are considered "security procedures" for purposes of Ohio Rev. Code § 1304.57; "[t]he term does not apply to procedures that the receiving bank may follow unilaterally in processing payment orders." *Id.* § 1304.56, official cmt. However, the agreement need not be a written contract. *Choice Escrow and Land Title, LLC v. BancorpSouth Bank*, 754 F.3d 611, 618 (8th Cir. 2014).

Woda entered into an ACH Agreement with Benchmark on March 28, 2011. The parties agreed to comply with the security procedures described in Schedule B of the Agreement. (¶

2(a), ECF No. 1-2). Schedule B provides that "any transaction initiated or authorized using a valid combination of a login ID and password will be considered authentic, valid, and binding" by the parties. (*Id.* Sched. B; George Depo., 73–74; Vincent Depo., 19). In addition to unique usernames and passwords for each authorized Woda employee, there is no dispute that Woda and Benchmark agreed to other security procedures for authenticating ACH transfers: a risk algorithm that triggered security challenge questions, account lockout after three unsuccessful login attempts, IP blacklisting, and dual authorization. (Banking Agreement, 2, ECF No. 1-3; George Depo., 75, 86, 92–93; Vincent Depo., 26, 36, 54; Vincent Decl., ¶ 6).

Accordingly, there is no genuine issue of material fact that Woda and Benchmark agreed that ACH payments would be verified pursuant to certain security procedures. The first part of the test under § 1304.57(B)(1) is satisfied.

2. Commercial Reasonableness of Benchmark's Security Procedures

Both sides primarily focus their arguments on the second part of the test—the commercial reasonableness of the security procedures just discussed. Ohio Rev. Code § 1304.57(B)(1)(a). According to Plaintiff,

> Benchmark did not act in a commercially reasonable manner because it: 1) failed to follow safe and sound policies ordered by the Federal Deposit Insurance Corporation ("FDIC") to safeguard the Limited Partnerships' deposits; 2) failed to provided multi-factor authentication for online banking, contra to the requirements of the Federal Financial Institutions Examination Council ("FFIEC"); 3) improperly and without authorization, gave Donna Ferrell access to the Limited Partnership accounts, even though her employment at Woda Construction, Inc. did not require her to have and/or need such access;[3] 4) failed to provide risk assessing monitoring of its depositors' accounts contra to the FDIC and FFIEC; and 5) improperly allowed customers to "opt-out" of security procedures, contra to FDIC and FFIEC requirements.[4]

[3] This is addressed in the next section.

[4] Plaintiff also argues that "Ohio law does not come into consideration here because Benchmark is federally regulated[.]" (Pl. Motion, 25). While Benchmark is undisputedly subject

(Pl. Motion, 4–5, ECF No. 53). Benchmark argues that "(1) the parties agreed to commercially reasonable security procedures, which the bank followed . . . [and] (2) the Limited Partnerships rejected additional commercially reasonable security procedures and expressly agreed to be bound by transfers made using its credentials." (Def. Motion, 11, ECF No. 51).

Pursuant to the Ohio Rev. Code § 1304.57(C)(1), the commercial reasonableness of a security procedure is determined by considering:

> (a) The wishes of the customer expressed to the bank;
> (b) The circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank;
> (c) Alternative security procedures offered to the customer;
> (d) Security procedures in general use by customers and receiving banks similarly situated.

The standard is not whether the security procedure is the best available but whether it is reasonable for the particular parties involved. U.C.C. § 4A-203, cmt 4. Moreover, a security procedure is *deemed* to be commercially reasonable if both of the following apply:

> (a) The security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer.
> (b) The customer expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer.

Ohio Rev. Code § 1304.57(C)(2). The issue of commercial reasonableness is a question of law. U.C.C. § 4A-203, cmt 4.

The Court first considers the "security procedures in general use by customers and receiving banks similarly situated." Ohio Rev. Code § 1304.57(C)(1)(d). While the Sixth Circuit

to federal regulation, the only remaining claim for relief is a violation of the Ohio Uniform Commercial Code. Ohio law clearly applies.

has not examined the issue, two Circuits that have analyzed security procedures in this context held that the use of a unique username and password alone is inadequate. *See Choice Escrow*, 754 F.3d 611, 620 (8th Cir. 2014); *Patco Const. Co., Inc. v. People's United Bank*, 684 F.3d 197, 210–11 (1st Cir. 2012). Taking it a step further, the First Circuit concluded that a security system using a unique username and password was not commercially reasonable when it was only backed up by challenge questions triggered by transfers exceeding $1.00. *Patco*, 684 F.3d at 210–11. According to the Court, this meant that customers who regularly initiated transfers were frequently answering their challenge questions, which "substantially increase[d] the risk of fraud." *Id.* at 210.

Both the First and Eighth Circuits applied the FFIEC's[5] guidance, cited by both parties here, when analyzing the commercial reasonableness of a bank's security procedures under nearly identical state statutes to Ohio's. *See Choice Escrow*, 754 F.3d at 619–20; *Patco*, 684 F.3d at 201. Aptly, the FFIEC Guidance states:

> "The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties . . . . Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks."

Patco, 684 F.3d at 201–02 (quoting FFIEC, Authentication in an Internet Banking Environment, 1–2 (Aug. 8, 2001), *available at* http://www.ffiec. gov/pdf/authentication_guidance.pdf)).

Relying on FFIEC guidance, the Eighth Circuit held that a dual authorization system

[5] The FFIEC was established to "prescribe uniform principles and standards for the Federal examination of financial institutions . . . and make recommendations to promote uniformity in the supervision of these financial institutions." 12 U.S.C. § 3301.

constituted a commercially reasonable security procedure because it added another layer of protection to a single level of authorization, such as a unique username and password. *Choice Escrow*, 754 F.3d at 620 (citing FFIEC, Authentication in an Internet Banking Environment (Oct. 12, 2005), *available at* https://www.ffiec. gov/pdf/authentication_guidance.pdf)). In fact, the Eighth Circuit noted that dual authorization may be more effective against certain types of internet fraud than multifactor authentication alone. *Id.* In other words, in a banking relationship like that at issue here, the FFIEC endorses the use of both layered security and multifactor authentication for high-risk transactions. (*See* Curtin Report, 6, ECF No. 51-5). The FFIEC explicitly states that the guidance does not exclusively call for the use of multifactor authentication or recommend multifactor authentication over layered security. FFIEC, Frequently Asked Questions, 2–3 (Aug. 15, 2006), *available at* https://www.ffiec.gov /pdf/authentication_faq.pdf.

Multifactor security includes the use of two of the following: something the user knows, something the user has, and something the user is. *Choice Escrow*, 754 F.3d at 620. Layered security can include a combination of single-factor authentication methods, such as "application timeouts with mandatory reauthentication, fraud detection and monitoring systems, dual customer authorization, and reputation-based tools to block connections to the institution's servers based on device or network indicators known or suspected to be associated with fraudulent activities." (Curtin Rep., 7, citing FFIEC, Information Security Booklet, 36 (September 2016) *available at* https://www.ffiec.gov/press/PDF/FFIEC_IT_Handbook _InformationSecurity_Booklet.pdf). Here, Benchmark implemented layered security by utilizing unique usernames and passwords, security challenge questions triggered by a risk algorithm, account lockout after three unsuccessful login attempts, IP blacklisting, and dual authorization.

Next, the Court considers the "alternative security procedures offered to the customer" and "the wishes of the customer expressed to the bank." Ohio Rev. Code § 1304.57(C)(1)(a),(c). In addition to the security procedures agreed to, Benchmark offered Woda the use of a manual report system and banking tokens. Both parties agree that banking tokens are a commercial reasonable security measure. (Hadley Aff., ¶ 16, ECF No. 53-4; Curtin Rep., 8). However, at Woda's request, Benchmark allowed Woda to reject the use of a manual report system and banking tokens (George Depo., 78–79, 102–03, 137–38), and to bypass dual authorization for select employees. (Vincent Decl., ¶ 7).

While Plaintiff's expert claims that the FFIEC rejects a customer's decisions to opt-out of security measures, this position is unsupported by the documentation Mr. Hadley references in his Report. Instead, the FFIEC explains that while customers should not be permitted to "opt-out" of additional authentication controls when the result is reliance on one single-factor authentication measure alone (i.e., unique username and password combination), "an institution may permit customers to choose between different authentication options provided the options offered are consistent with the guidance." (FFIEC, Frequently Asked Questions, 4–6). Layered security, even without dual authorization, is consistent with the FFIEC Guidance. (Curtin Rep., 7, citing FFIEC, Information Security Booklet, 36).

Finally, the Court moves to the fourth factor—"the circumstances of the customer known to the bank." Ohio Rev. Code § 1304.57(C)(1)(b). While "[a] receiving bank might have several security procedures that are designed to meet the varying needs of different customers[,]" it is not required. U.C.C. § 4A-203, cmt 4. It is not *per se* commercially unreasonable for a bank to use a single effective and versatile security protocol for the majority of its customers and depart from the protocol only when necessary. *Choice Escrow*, 754 F.3d at 621. A bank's generic one-size-fits all approach to customers only violates Article 4A if it does not take a customer's specific circumstances into account. *Patco*, 684 F.3d at 212.

Here, Mr. Woda and Mr. Cooper served dual roles: sitting on the Benchmark Board of Directors and acting as managing directors of Woda. (Caldwell Decl., ¶ 3). Accordingly, they were in the unique position of being able to participate in establishing Benchmark's general security policies for ACH transfers with Woda's unique circumstances in mind. (Vincent Depo., 44, 65; Ex. B, ECF No. 44-2; Decl. Caldwell, ¶ 9). And there is no dispute that when the general security protocol did not suit Woda's circumstances, Benchmark altered it to fit the needs of the customer: Benchmark allowed Woda to utilize only the online banking system for ACH transfers, to reject banking tokens as "inconvenient," and to bypass dual authorization for select employees. (Vincent Decl., ¶ 7; George Depo., 78–79, 102–03, 137–38).

The Court finds that Benchmark's security procedures were commercially reasonable as a matter of law pursuant to Ohio Rev. Code § 1304.57(C)(1).[6] Moreover, Woda ultimately "agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure[s] chosen by the customer." (*See* ACH Agreement, Sched B, "[A]ny transaction initiated or authorized using a valid combination of a login ID and password will be considered authentic, valid, and binding by the Company and Benchmark Bank."); Ohio Rev. Code § 1304.57(C)(2)(b). Thus, § 1304.57(C)(2) also applies. *See also* U.C.C. § 4A-203, cmt 4 (explaining that the risk of loss shifts to the customer where the informed customer refuses security procedures that are commercially reasonable and suitable for

[6] Plaintiff's continued references to two FDIC Consent Orders (ECF Nos. 53-7–9) regarding "unsafe banking practices" are irrelevant to this issue. Both Orders address shortcomings regarding Benchmark's capitalization and asset management. Similarly, Plaintiff's repeated discussions regarding "risk analysis security" are also immaterial.

the customer and insists on using higher-risk procedures because they are convenient). Pursuant to Ohio Rev. Code § 1304.57(B)(1)(a), the second part of the test is satisfied.

3. Benchmark's Good Faith and Compliance with ACH Agreement and/or Woda's Instructions

Under the third part of the test, Benchmark must also prove that it accepted the fraudulent payment orders "in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer." Ohio Rev. Code § 1304.57(B)(1)(b).

"Good faith" means "honesty in fact and the observance of reasonable commercial standards of fair dealing." *Id.* §§ 1301.201(B)(20), 1304.51(A)(9). This definition has both a subjective ("honesty in fact") and objective component ("observance of reasonable commercial standards"). *In re Nieves,* 648 F.3d 232, 239 (3d Cir. 2011); *In re Jersey Tractor Trailer Training, Inc*., 580 F.3d 147, 156 (3d Cir. 2009). There is nothing in the record to suggest that Benchmark did not accept the payment orders honestly, so the Court will focus on the objective prong.

Having already examined the commercial reasonableness of Benchmark's security procedures, "[t]he objective good faith inquiry concerns a bank's acceptance of payment orders in accordance with those security procedures" and any written agreement or instruction of the customer. *Choice Escrow*, 754 F.3d at 623. However, "technical compliance . . . is not enough under Article 4A; instead . . . the bank must abide by its [security] procedures" and any written agreements or instructions of the customer "in a way that reflects the parties' reasonable expectations . . . as established by reasonable commercial standards of fair dealing." *Id; see also In re Nieves,* 648 F.3d at 239–40 (explaining that the objective good-faith standard deals with what a party knew or should have known, taking into consideration the customary practices of the industry).

Woda was aware that pursuant to the ACH Agreement executed between the parties, the purpose of the security procedures in place was "for verification of authenticity and not to detect an error in the transmission or content of an Entry." (ACH Agreement, ¶ 2(a)). Thus, Woda knew that Benchmark employees were not checking whether a receiving entity had a relationship to or prior history with Woda, whether a recipient's name was of Eastern European origin, or where an originating IP address was located. (Pl., Motion, 10, 26); *see Choice Escrow,* 754 F.3d at 623 ("[The customer] was also aware that the role of those [bank] employees was not to check for any irregularities but to route these payment orders to the correct beneficiaries.").

In fact, according to Ms. Vincent, she processed the fraudulent transfers the same way she processed all ACH transfers: she looked to see if the ACH transfer was generated by a known authorized user, the debts and credits balanced, and the account the user was transferring money from had money in it to cover the transfer. (Vincent Depo., 31, 179). Similarly, Fiserv verified that Ms. Ferrell's username, password, and security questions, if prompted, were correct when the fraudulent transfers were made. (*Id.* at 36). The transfers were not initiated from IP addresses that were blacklisted, and on Benchmark's end, there was no notice of an account lockout. (*Id.* at 139–40; Ex. B, ECF No. 52-1). Accordingly, there is no dispute that Benchmark acted according to the reasonable expectations of the parties in following the established security procedures.

However, there are genuine issues of material fact concerning whether Benchmark accepted the fraudulent ACH transfers pursuant to the ACH Agreement and/or Woda's instructions. The first two disputes involve whether the ACH Agreement was modified. The ACH Agreement states that "[n]o course of dealing between Benchmark Bank and Company will constitute a modification of this Agreement . . . or constitute an agreement between the Benchmark Bank and Company regardless of whatever practices and procedures Benchmark Bank and Company may use." (¶ 25, ECF No. 1-2). However, under Ohio law, notwithstanding the terms of a written agreement, "oral modification of a written contract can be enforceable" where "the parties have engaged in a course of conduct in conformance with the oral modification." *Exact Software N.A., Inc. v. Inforcon Systems, Inc*., No. 3:03CV7183, 2004 WL 952876, at *5 (N.D. Ohio Apr. 16, 2004); *Smaldino v. Larsick*, 630 N.E.2d 408, 412–13 (Ohio Ct. App. 11th Dist. 1993).

The written ACH Agreement lists the maximum limit for a single ACH transfer for Woda as $50,000. (ACH Agreement, Sched C). Six of the fraudulent transfers initiated between May 18 and May 24, 2016, exceeded this limit. (Woda Aff., ¶¶ 15–27). For example, the third fraudulent ACH transfer initiated from the Boury Lofts account was for $83,217.00. (*Id.* at ¶ 23). According to Ms. George, who is listed as Woda's authorized representative in the ACH Agreement, she was not aware of any amendment to Schedule C. (Scheds. B, C, ECF No. 1-2; George Depo., 105–06). This is disputed by Ms. Vincent's testimony that it was not unusual for Woda associates to make ACH transfers as large as and larger than the amounts fraudulently transferred. (Vincent Decl., ¶ 14, according to Ms. Vincent, Ms. Ferrell made a legitimate transfer from the WCI account on May 19, 2016 for $2,419,540.14).

Similarly, Schedule C of the ACH Agreement lists the Woda accounts that were allowed access to ACH services at the time of the signing of the Agreement. (ACH Agreement, Sched C). The Limited Partnerships are not listed. (Woda Aff., ¶ 10). Again, Ms. George was not aware of any amendments to Schedule C. (George Depo., 105). Yet, Mr. Caldwell contends that there was an "understanding" between Benchmark and Woda that the ACH Agreement would apply to all

Woda entities and affiliates that banked at Benchmark and requested ACH services, including the Limited Partnerships. (Caldwell Decl., ¶ 8; Vincent Depo., 89–92). According to Ms. Vincent, there did not need to be a new or updated agreement each time an authorized account was added—all new Woda accounts opened after March 28, 2011, including the Limited Partnerships, were covered by the original ACH Agreement. (Vincent Depo., 89–92). While Ms. George assumed that if a new account was set up, it was "set up to be in line with all of the other . . . preexisting accounts," (George Depo., 106), it is unclear where this "understanding" came from. Thus, disputes of fact exist as to whether Benchmark engaged in a course of conduct in conformance with oral modifications to the ACH Agreement to include the maximum amount allowed to be transferred and what accounts were included in Schedule C.

Finally, while it is undisputed that the fraudulent ACH transfers were made using Ms. Ferrell's username and password, Plaintiff argues that Woda never authorized Benchmark to give Ms. Ferrell access to the Limited Partnership accounts. The record on this is less than clear.

On March 22, 2016, Ms. Clifford e-mailed Ms. Vincent requesting that Ms. Ferrell, who had just replaced Sue Milner at Woda, be given access to view and process ACH transfers for WCI. (Ex.7, ECF No. 46-4). Ms. George also told Ms. Vincent to "duplicate Sue's rights with respect to activities that she could perform, but not necessarily access rights to properties that Sue had access to." (*Id.*). It is unclear what this statement is referring to and there is no evidence about what Sue's rights had been. Nevertheless, with Woda's approval, Ms. Ferrell did have the ability to bypass dual authorization and initiate and approve ACH transfers for processing. (George Depo., 121–23; Ex. 8, ECF No. 46-5).

According to Ms. Vincent, prior to the fraudulent transfers, she was asked to designate the Limited Partnership accounts as "construction accounts" with both online banking and ACH access and to give the entire Woda accounting group access to the accounts. (Vincent Decl., ¶¶ 8–9). Ms. Vincent also claims that Ms. Clifford and Ms. George specifically requested by telephone that Ms. Ferrell be given ACH access to the Limited Partnership accounts. (*Id.* ¶ 11; Vincent Depo., 105–07). However, Ms. George contends that neither she nor anyone at Woda authorized Benchmark to give Ms. Ferrell access to the Limited Partnership accounts, "much less the ability to process ACH transfers from these accounts." (George Aff., ¶ 14). Thus, there is a genuine dispute as to whether Ms. Ferrell should have had access to process ACH transfers from the Limited Partnership accounts.

Because the Court is left with these disputes, genuine issues exist regarding whether Benchmark accepted the payment orders in good faith and in compliance with the ACH Agreement and/or Woda's instructions. *See Experi-Metal*, 2010 WL 2720914, at *7–8 (denying summary judgment because questions of fact remained as to whether the bank acted in good faith where there was evidence in the record that the bank disregarded the customer's verbal instructions). Resolutions of these factual issues will require a credibility determination by the Court and such determination is not appropriate on a motion for summary judgment, even where there is no jury demand. *TransWorld Airlines, Inc. v. Am. Coupon Exch., Inc.*, 913 F.2d 676, 684–85 (9th Cir. 1990). Accordingly, the Court cannot determine whether the third part of the test under Ohio Rev. Code § 1304.57(B)(1)(b) is satisfied and ultimately whether the payments at issue were verified.

C. Plaintiff's Entitlement to Refund

If the Court finds that Benchmark failed to verify the fraudulent payments pursuant to Ohio Rev. Code § 1304.57(B), "the bank shall refund any payment of the payment order received from the customer . . . and shall pay interest on the refundable amount calculated from the date the bank received payment to the date of the refund." *Id.* § 1304.59. If the Court finds that Benchmark did verify the fraudulent payments pursuant to § 1304.57(B), the bank is still required to refund the customer if either of the following exceptions apply:

> (1) By express written agreement, the receiving bank may limit the extent to which it is entitled to enforce or retain payment of the payment order.
>
> (2) The receiving bank may not enforce or retain payment of the payment order if the customer proves that the order was not caused, directly or indirectly, by either of the following:
>
> > (a) A person entrusted at any time with duties to act for the customer with respect to payment orders or the security procedure;
> >
> > (b) A person who obtained access to transmitting facilities of the customer or who obtained, from a source controlled by the customer and without authority of the receiving bank, information facilitating breach of the security procedure, regardless of how the information was obtained or whether the customer was at fault.

Id. § 1304.58(A)(1), (2). The Court will discuss each exception in turn.

1. Agreement by Benchmark to Limit Enforcement of Payment

Under the first exception, a bank is required to refund a customer for an unauthorized payment order, even if the payment was verified pursuant to § 1304.57(B), if the bank agreed to take all or part of the loss resulting from the unauthorized payment order. U.C.C. § 4A-203, cmt 6.

Although Plaintiff cites to a clause in the Banking Agreement that seems to limit Woda's loss to $500 for unauthorized transfers, Plaintiff ignores the applicable language of the ACH Agreement. Paragraph 25 of the ACH Agreement provides that "[i]n the event of any inconsistency between the terms of this Agreement and the Account Agreement, the terms of this Agreement shall govern." (ECF No. 1-2). Paragraph 3(a) of the ACH Agreement explicitly states:

> If an Entry . . . received by Benchmark Bank purports to have been transmitted or authorized by Company, it will be deemed effective as Company's Entry . . . and

> Company shall be obligated to pay Benchmark Bank the amount of such Entry even though the Entry . . . was not authorized by Company, provided Benchmark Bank accepted the entry in good faith and acted in compliance with the security procedures referred to in Schedule B with respect to such entry.

(*Id.*). In other words, Benchmark limited its ability to enforce payment for unauthorized payment orders to only those that Benchmark verified pursuant to Ohio Rev. Code § 1304.57(B)(1)(b).

For the reasons previously discussed, questions of fact remain as to whether Benchmark accepted the fraudulent transfers in good faith. Accordingly, if the Court determines at trial that Benchmark accepted the fraudulent transfers in good faith, paragraph 3(a) of the ACH Agreement provides that the risk of loss stays with Plaintiff. If the Court determines the opposite, this provision is inapplicable; the risk of loss shifts to Benchmark because the payments are unverified under Ohio Rev. Code § 1304.57(B).

2. Woda's Role in Security Breach

Under the second exception, a bank is required to refund a customer, even if the payment was verified pursuant to § 1304.57(B), if the customer can prove that the culprit did not obtain confidential security information controlled by the customer. U.C.C. § 4A-204, cmt 1. In other words, "[i]f the customer can prove that the person committing the fraud did not obtain the confidential information from an agent or former agent of the customer or from a source controlled by the customer, the loss is shifted to the bank." *Id.* § 4A-203, cmt 5. "Prove" is defined as "to meet the burden of establishing the fact." Ohio Rev. Code § 1304.51(A)(14).

After examining Ms. Ferrell's computer, Woda's IT Technician e-mailed Mr. Cooper and alerted him that malware of an unknown type was found on Ms. Ferrell's computer. (Ex. 15, ECF No. 47-5). Based on review of the log activity, Fiserv also believed there was malware in Woda's network, which allowed the attackers to obtain valid credentials for use in the ACH origination and authorization. (Ex. B, ECF No. 52-1). According to Fiserv, they confirmed that they did not detect any user ID or password data breach on their network nor did they have any records of recent accounts with stolen credentials from customers. (*Id.*). Moreover, monthly vulnerability and penetration testing did not detect any intrusions. (*Id.*).

After the attack, Woda hired Rook to conduct a forensic investigation and network vulnerability analysis of Woda's computer systems. (Ferrell Depo., 51, 57). In Rook's Vulnerability Analysis Report, it identified, among other things, that "two hosts were found running IPMI v.2.0 which contains an information disclosure vulnerability, allowing attackers to obtain password hashes." (Ex. 16, p. 19, ECF No. 47-6). Rook classified this internal environment vulnerability as "high risk." (*Id.*).

Despite all of this, Plaintiff's expert, Mr. Hadley, believes the "criminals got everything they needed from eavesdropping network traffic between Benchmark and their depositors"—specifically Benchmark's unencrypted e-mails to Woda, which included online banking usernames and generic temporary passwords for new accounts. (Hadley Report, 2, 6–7, ECF No. 51-5). However, there is no evidentiary support for Mr. Hadley's belief.

In fact, the undisputed evidence undermines Mr. Hadley's belief. At the time of the fraudulent transfers, Ms. Ferrell's password was not "woda123," "woda2013," "bench123," "bench456," "bench2012," "bench4567," or "belh2105," which were the only (temporary) passwords transmitted by e-mail. (Ex. G, ECF No. 43-8). Rather Ms. Ferrell's Benchmark account password was "Cincy24!" which was known only to Ms. Ferrell and kept on a sticky note in a locked drawer in Ms. Ferrell's office. (Ferrell Depo., 28). Immediately after being told she was locked out of her account on her own computer, Ms. Ferrell was able to log in to her Benchmark account on Ms. Myers' computer and process an ACH transfer. (Ferrell Depo., 34–38). Ms. Ferrell was also able to log back into her Benchmark account on her own Woda computer on May 19 using the same username and password she had previously been using. (Ferrell Depo., 38). Thus, Mr. Hadley's suggestion that Ms. Ferrell's access to her Benchmark account was compromised by an unauthorized person who set up a new username, password, and security questions unknown to Ms. Ferrell as a result of these unencrypted e-mails is unsupported. (Hadley Rep., 2, 6–7). Moreover, while Mr. Woda and Mr. Cooper may not have liked or agreed with the findings of the security firm they hired to evaluate Woda's computer system, their opinions do not negate Rook's or Fiserv's findings in the face of no admissible evidence to the contrary. (Ex. 17, ECF No. 48-2).

Thus, there is no genuine issue of material fact that Woda has not established that the person who committed the fraudulent payment orders did not obtain the confidential information from a source controlled by Woda. Accordingly, if the Court determines at trial that the Bank accepted the fraudulent transfers in good faith, the risk of loss stays with Plaintiff.

D. Indemnification Clauses

Benchmark argues that if Plaintiff's claim survives summary judgment, Benchmark is entitled to its affirmative defense of setoff for its attorneys' fees and costs in both lawsuits pursuant to indemnity clauses located at paragraphs 13 and 14 of the ACH Agreement.

"A setoff is defined as 'that right which exists between two parties, each of whom under an independent contract owes a definite amount to the other, to set off their respective debts by way of a mutual deduction.'" *Beck v. Mar Distribs. of Toledo, Inc*., 2012-Ohio-5831165, 2012 WL 5831165, at *2 (Ohio Ct. App. 6th Dist. 2012) (quoting *Witham v. South Side Bldg. & Loan Ass'n of Lima, Ohio*, 15 N.E.2d 149, 150 (Ohio 1939)).[7] An important element of the right to

[7] The Agreements at issue in this case contain an Ohio forum selection clause, both parties rely on Ohio law, and the entire relationship between the subrogor and Defendant took place in Ohio. Accordingly, Ohio law applies to Benchmark's affirmative defense. *Int'l Ins. Co.*

setoff is mutuality of obligation—both parties to the lawsuit are also parties to the independent contract on which the right to setoff is claimed. *Id.* "In contrast to recoupment, a setoff is 'a demand asserted to diminish or extinguish a plaintiff's demand, which arises out of a transaction different from that sued on, and which must be liquidated and emerge from a contract or judgment.'" *American Motorists Ins. Co. v. Olin Hunt Specialty Products, Inc.*, 2001 WL 1098013, at *3 (Ohio Ct. App. 10th Dist. 2001) (quoting *Continental Acceptance Corp. v. Rivera,* 363 N.E.2d 772, 776 n.17 (Ohio 1976)).

There is no dispute that the parties to the ACH Agreement are Woda and Benchmark Bank. However, because subrogation is "[t]he substitution of one person in place of another with reference to a lawful claim, demand, or right[,]" Plaintiff stands in the shoes of Woda. *American Motorists*, 2001 WL 1098013, at *3 (quoting *American Ins. Group v. McCowin,* 7 Ohio App. 2d 62, 65 (Ohio 1966)). And in the same way that Federal can act as the subrogee of the Limited Partnerships in its comprehensive coverage of Woda in bringing this action, there is mutuality of obligation between Federal and Benchmark. (*See* Phair Aff., ¶ 3).

The second indemnification clause in the ACH Agreement states:

> Company agrees to indemnify Benchmark Bank against any loss, liability or expense (including attorney's fees and expenses) resulting from or arising out of any claim of any person that the Benchmark Bank is responsible for any act or omission of Company or any other person described in this Section[.]

(¶ 14(a), ECF No. 1-2).

The commentary of the applicable federal regulation "establishes that [U.C.C.] Article 4A [(adopted by Ohio Revised Code Chapter 1304)], governing Fedwire funds transfers, 'supersedes or preempts inconsistent provisions of state law.'" *Texas Brand Bank v. Luna &*

v. Stonewall Ins. Co., 86 F.3d 601, 604 (6th Cir. 1996); *Ohayon v. Safeco Ins. Co. of Ill*., 747 N.E.2d 206, 209, 210 (Ohio 2001).

Luna, LLP, No. 3:14-CV-1134-P, 2015 WL 12916411, at *5 (N.D. Tex. Feb. 27, 2015) (quoting Comm. on § 210.25, 12 C.F.R. Part 210, Subpt. B, App. A (2015)). While the Sixth Circuit has not spoken on the scope of the regulation's preemption, the Fourth Circuit has determined that a state law claim is preempted if "the challenged conduct in the state claim would be covered under Subpart B as well." *Eisenberg v. Wachovia Bank, N.A.*, 301 F.3d 220, 223 (4th Cir. 2002). The Eighth Circuit also determined that U.C.C. Article 4A preempts common law causes of action "where the common law claims would create rights, duties, or liability inconsistent with [Article 4A]; and . . . where the circumstances giving rise to the common law claims are specifically covered by [Article 4A]." *Choice Escrow*, 754 F.3d at 625.

In a similar action under Missouri's identical adaptation of the U.C.C. provisions at issue, the Eighth Circuit held that the bank's counterclaim to enforce a similar indemnification provision, where the bank sought only attorney's fees, was not inconsistent with U.C.C. Article 4A because Article 4A "contains no provision allocating attorney's fees between the bank and the customer in the event of litigation." *Id.* at 626. The Court went onto explain that "[a]lthough awarding attorney's fees to bank under an indemnification agreement might reduce a customer's overall recovery against that bank, it would do so for reasons extrinsic to Article 4A's attempts to balance the risk of loss due to a fraudulent payment order." *Id.* Moreover, there are no specific public policy exceptions that prevent the enforcement of an indemnification clause under Ohio Revised Code Chapter 1304. *Worth v. Aetna Cas. & Sur. Co.*, 513 N.E.2d 253, 257 (Ohio 1987) ("In the absence of specific public policy exceptions . . . an agreement to indemnify another is generally enforceable.").

Finding *Choice Escrow* to be the only Circuit authority directly on point, the Court concludes that should Plaintiff prevail at trial, Benchmark may seek to setoff its reasonable attorneys' fees and court costs for both lawsuits, pursuant to Paragraph 14 of the ACH Agreement.[8]

IV. CONCLUSION

For the foregoing reasons, the Court **DENIES IN PART** and **GRANTS IN PART** Benchmark's Motion for Summary Judgment (ECF No. 51) and **DENIES** Plaintiff's Motion for Summary Judgment. (ECF No. 53).

In sum, if the Court determines at trial that Benchmark did not accept the payment orders in good faith and in compliance with the ACH Agreement and/or Woda's instructions, the loss of $403,196.00 plus interest shifts to Benchmark. However, Benchmark may seek to recover its reasonable attorneys' fees and costs from Plaintiff for both lawsuits. If the Court determines at trial that Benchmark accepted the payment orders in good faith and in compliance with the ACH Agreement and/or Woda's instructions, the loss will stay with Plaintiff, as Woda's subrogee.

An Order scheduling this case for a bench trial will be forthcoming.

IT IS SO ORDERED.

/s/ Sarah D. Morrison
SARAH D. MORRISON
UNITED STATES DISTRICT JUDGE

[8] Given this conclusion, the Court does not address the indemnification clause at paragraph 13 of the ACH Agreement, which appears to be more problematic. *See Texas Brand*, 2015 WL 12916411, at *5.